ABSTRACT OF THE DISCLOSURE

A method for power reduction and increasing computation speed for a Montgomery modulus multiplication module for performing modulus multiplication. A coding scheme reduces the hamming distance for partial product and multiple modulus selection, reducing MUX operations and power consumption. Synchronization registers synchronize partial product and multiple modulus values input to an accumulator reducing glitch and/or increase computation speed. Registers provide storage of previous values and reduce the need to obtain the values from a MUX, reducing MUX operations and/or reducing power consumption.